УДК 681.518.54

СПОСІБ УНІФІКАЦІЇ ФОРМ ПОДАННЯ ЗНАНЬ В ЕКСПЕРТНИХ СИСТЕМАХ

Ярослав Провотар
Національний Технічний Університет України "КПІ"

Анотація: **В роботі розглянуто один із методів вирішення проблеми уніфікації форм подання знань в експертних системах. Пояснення методу приводиться на прикладі двох задач, пов'язаних з різними сферами людської діяльності, вирішення яких можливе за допомогою єдиного програмного комплексу**
Summary: **One of the ways solving the knowledge form unification problem in expert systems on the example of two sums, connected with different branches of knowledge, which can be solved using one programming complex, is considered in this work**

На сучасному етапі розвитку технологій експертні системи починають користуватися попитом в доволі різних сферах людської діяльності. Внаслідок цього зросли вимоги до експертних систем, які за таких умов мають обробляти інформацію, пов'язану з абсолютно різними галузями знань. Ці вимоги спричинили появу проблеми уніфікації форм знань в експертних системах, і тим самим універсалізації програмного забезпечення для роботи з базами знань. В повній мірі зробити унівенсальну систему, яка б забезпечувала обробку інформації в довільній галузі знань для довільних задач, є неможливим. Тому має зміст уніфікації форм подання знань для певного класу задач, які можуть бути загальними для багатьох сфер людської діяльності. В доповіді буде розглянуто клас задач, який є загальним для таких галузей знань, як захист інформації, медицина та інших.

Розглянемо дві задачі, які існують в різних сферах людської діяльності: задача діагностики ступеню захищеності інформації в сфері інформаційної безпеки та задача діагностики захворювань в сфері медицини. В обох випадках є *об'єкт дослідження* (наприклад офіс, чи інший об'єкт, ступінь інформаційної захищеності якого досліджується, - в сфері інформаційної безпеки, чи людський організм - в сфері медицини). Об'єкт дослідження має певні *характеристики*, які потребують визначення для подальшого аналізу (наприклад наявність комп'ютерного обладнання на об'єкті чи група крові). Для кожного об'єкту дослідження у відповідності до задачі існують *типи загроз* (наприклад викрадення інформації за допомогою засобів візуального спостереження чи онкологічні захворювання) та *засоби загрози* (наприклад відеокамери чи збудники захворювань), які можуть діяти на нього, а звідси і *засоби захисту* об'єкту від загроз (наприклад засоби обмеження бачення чи медичні препарати). Тим самим описано кінцевий набір термінів, з яким можна починати процес експертизи.

Процес експертизи починається з'ясуванням усіх характеристик об'єкту дослідження, необхідних для подальшого аналізу. Після цього, виходячи з визначених характеристик, робиться висновок, які типи загроз є найбільш імовірними. Для кожного типу загроз робиться вибір засобів реалізації загрози, які можуть бути використані проти об'єкту дослідження. Виходячи з типів та засобів реалізації загрози робиться вибір засобів захисту, з метою зниження імовірності здійснення загрози до мінімуму. Кінцевим результатом експертизи є оцінка імовірності здійснення загрози в відсотках, а також рекомендації щодо зменшення цієї імовірності до мінімуму. Як можна помітити, запропоновану схему експертизи неможливо впровадити, використовуючи лише логічні вирази (наприклад предикати), які впливають лише на послідовність процесу експертизи, тому при реалізації такої схеми мають бути використані і арифметичні вирази – формули, за допомогою яких виробляються кількістні оцінки імовірності здійснення загрози для кожної характеристики об'єкту дослідження, а також сукупна імовірність здійснення загрози для об'єкту дослідження у цілому. Тим самим отримується арифметико-логічна схема експертизи, яка має широкий діапазон використання в практично довільних сферах людської діяльності.

Як видно з прикладу, обидві задачі мають однаковий набір термінів, отже можуть бути реалізовані в одному програмному комплексі. Не важко помітити, що така схема опису об'єкта дослідження, а також процесу експертизи, підходить для багатьох задач в інших галузях знань. Тим самим досягається певний рівень універсальності при побудові та використанні баз знань в експертних системах. Ця модель побудови баз знань та процесу експертизи була використана при розробці експертної системи оцінки інформаційної захищеності об'єкту, яка була спроектована на кафедрі спеціалізованих комп'ютерних систем НТУУ "КПІ". При цьому були розроблені схеми побудови предикатів та формул з урахуванням якомога більшої кількості вимог до баз знань. В результаті цього схема побудови предикатів відповідає загальній схемі побудови експертиз – структури, яка має

вигляд логічного дерева, і яка може бути зручно приведена до системи логічних формул, які мають механізм оптимізації та скорочення. Схема побудови формул має практично універсальний набір функцій та констант, за допомогою яких можливий опис формули довільної складності з довільною кількістю аргументів. Тим самим за допомогою схем побудови предикатів та формул можливий опис предикатів та формул для довільного факту з довільної галузі знань. Отже експертна система оцінки інформаційної захищенності об’єкту має високий ступінь унівенсальності і може бути з успіхом застосована для вирішеня класу задач діагностики та покращення стану захищеності об’єкту дослідження від загроз в доволі великій кількості сфер діяльності людини, таких як медицина, захист інформації, спорт, психологія та інших.

УДК 681.518.54

АЛГОРИТМІЧНІ ОСОБЛИВОСТІ ЕКСПЕРТНИХ СИСТЕМ, ОРІЄНТОВАНИХ НА ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Денис Замятін, Михайло Прокофьєв

Національний Технічний Університет України “КПІ”

Анотація: **Доклад присвячено проблемам та особливості реалізації і використання експертних систем в області захисту інформації. Розглянуті методи забезпечення конфіденційності даних щодо конфігурації об’єкту, який досліджується. Особлива увага приділена питанням розробки блоку виведення нових знань.**

Summary: **The report is devoted to problems and features of realization and using of expert systems in branch of guard. Is examined methods of guarantee confidentiality of data about investigated object and peculiarities of development of block derivation of new knowledge.**

В сучасних умовах інформація є одним із найважливіших та найдорожчих ресурсів. У такій ситуації особливо актуального значення набуває задача оцінки імовірності витоку інформації для певного об’єкта і пошуку методів підвищення інформаційної захищенноті цього об’єкта. Розв’язання цієї задачі традиційними методами пов’язане з цілим рядом труднощів, як економічного, так і психологічного характеру. Одним із шляхів підвищення ефективності процесу оцінки захищеності об'єкта є створення відповідних комп'ютерних систем. В зв’язку з тим, що при аналізі інформаційної захищеності об'єкта необхідно брати до уваги велику кількість непов'язаних між собою чинників, реалізація такого аналізу є нетривіальною задачею, що складно формалізується. Для розв’язання такого роду задач найбільш продуктивним виявляється використання систем із штучним інтелектом, зокрема експертних систем.

Експертна система збирає інформацію про об'єкт, що досліджується, задаючи питання користувачеві. Відповіді користувача перетворюються в логічні константи, що відповідають певним фактам. На підставі цієї інформації виводяться нові знання про об'єкт, такі як імовірність витоку інформації і т.п.

Досвід розробки і застосування подібних систем дозволив визначити ряд специфічних проблем і алгоритмічних особливостей, характерних для галузі захисту інформації.

Інформація про об'єкт, що досліджується, представляється у вигляді сукупності логічних фактів. Оскільки ситуація на об'єкті звичайно динамічно змінюється, користувач може бути зацікавлений у можливості модифікувати значення вже зібраних фактів або додавати нові. Для реалізації такої можливості система має бути здатна зберігати базу даних на магнітних носіях. База даних сама по собі може бути об'єктом нападу зловмисників, оскільки вона містить практично всю інформацію про засоби і заходи захисту, використані на об'єкті, що досліджується. Тому сама база має бути надійно захищена від несанкціонованого доступу шляхом шифрування. Система має бути здатна идентифікувати користувача, що працює з нею, і дозволяти йому працювати тільки зі своїми базами.

Як зазначалося вище, вся інформація про об'єкт подана як сукупність фактів, слабо пов'язаних між собою. Тому, крім звичайних методів виведення, система повинна мати механізм послідовного встановлення ряду фактів. Цей механізм може бути реалізований у вигляді ряду ключових точок, що відображують певні стадії процесу виведення.

Для повноцінної роботи системи недостатньо двох стандартних логічних значень фактів. Крім того, що значення факту може бути істинним або хибним, мають бути додаткові варіанти для відображення ситуації, коли користувач не знає відповіді або система не здатна встановити факт. У зв'язку з цим необхідно розробити спеціальний розширений логічний тип даних. Для такого типу повинні бути спеціально модифіковані стандартні булеві функції, які коректно працюють зі значеннями, що були додані.